AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application:

1. (Currently Amended) A multi-function peripheral device comprising:

a network interface configured to allow the multi-function peripheral device to communicate with network devices over a network;

a graphical user interface configured to allow for the exchange of information between the multi-function peripheral device and a user, wherein the information comprises configuration data for a virus protection process that includes attributes that the user specifies to configure the virus protection;

one or more processors;

a memory;

a scan process configured to scan one or more documents at the multi-function peripheral device;

a print process configured to print one or more documents at the multi-function peripheral device; and

the virus protection process executing in the memory and being configured to perform the steps of:

examine data stored on non-volatile memory of the multi-function peripheral device based upon the configuration data for the virus protection process;

based on examining the data, detect that one or more unauthorized instructions are stored on the non-volatile memory of the multi-function peripheral device; and

in response to detecting that the one or more unauthorized instructions have been stored on the non-volatile memory of the multi-function peripheral device:

perform one or more actions to address the one or more unauthorized instructions that have been stored on the non-volatile memory of the multi-function peripheral device based upon the configuration data for the virus protection process.

2. (Previously Presented) The multi-function peripheral device as recited in Claim 1, wherein the virus protection process is configured to detect that the one or more unauthorized instructions have been stored on the multi-function peripheral device by periodically examining, according to the configuration data, data stored on the multi-function peripheral device to determine whether the data has been modified in an unauthorized manner.

3. (PREVIOUSLY PRESENTED) The multi-function peripheral device as recited in Claim 1, wherein the virus protection process is configured to detect that the one or more unauthorized instructions have been stored on the multi-function peripheral device by examining and detecting the modification of data stored on the multi-function peripheral device, wherein the data is selected from the group consisting of one or more data files, program code, and configuration data.

4-7. (CANCELLED)

8. (ORIGINAL) The multi-function peripheral device as recited in Claim 1, wherein the virus protection process is further configured to undo changes made as a result of execution of the one or more unauthorized instructions.

9. (PREVIOUSLY PRESENTED) The multi-function peripheral device as recited in Claim 1, wherein the virus protection process is further configured to:

determine whether particular data stored on the multi-function peripheral device can be restored to a prior state; and

in response to determining that the particular data cannot be restored to the prior state, then delete the particular data from the multi-function peripheral device.

10. (CANCELLED)

11. (PREVIOUSLY PRESENTED) The multi-function peripheral device as recited in Claim 1, wherein the virus protection process is further configured to provide a notification that

the storage of the one or more unauthorized instructions on the multi-function peripheral device has been detected, wherein the notification is selected from the group consisting of displaying information on the graphical user interface on the multi-function peripheral device, printing a report on the multi-function peripheral device, sending an email from the multi-function peripheral device, and sending a facsimile from the multi-function peripheral device.

12-14. (CANCELLED)

15. (PREVIOUSLY PRESENTED) The multi-function peripheral device as recited in Claim 1, wherein the multi-function peripheral device is configured to receive, over a network, data used by the virus protection process to detect that the one or more unauthorized instructions have been stored on the multi-function peripheral.

16. (PREVIOUSLY PRESENTED) The multi-function peripheral device as recited in Claim 1, wherein:

the one or more unauthorized instructions are contained in a file stored on a portion of the non-volatile memory;

the one or more actions includes deleting the file; and

the virus protection process is further configured to, after deleting the file, overwrite the portion of the non-volatile memory with a specified pattern.

17-28. (CANCELLED)